embodiments and/or the dependent claims with the features of the independent claims, and not solely the combinations explicitly set out in the claims.

[0128] It is also noted herein that while the foregoing describes example embodiments of the invention, these descriptions should not be viewed in a limiting sense. Rather, there are several variations and modifications which may be made without departing from the scope of the present invention as defined in the appended claims.

1-34. (canceled)

35. A method in a cellular terminal, comprising:

transmitting a request that requires authentication procedure triggering to a cellular network and responsively receiving from the cellular network an authentication request message with an indication of a selected cryptographic algorithm from a group of a plurality of cryptographic algorithms;

attempting to decode the authentication request message to a decoded authentication request according to the selected cryptographic algorithm and based on a shared secret known by the cellular terminal and a network operator of the cellular terminal;

producing a determination whether the attempt was successful and the cellular terminal supports the selected cryptographic algorithm in authenticating to the cellular network; and

in case the determination is positive, based on the decoded authentication request, the shared secret and the selected cryptographic algorithm, producing and encrypting an authentication response message and transmitting the authentication response message to the cellular network; and

in case the determination is not positive, producing and sending to the cellular network a failure report.

36. The method of claim **35**, wherein the request that requires authentication procedure triggering is selected from a group consisting of: a network registration request; a routing area request; and a tracking area update request.

37. The method of claim **35**, wherein the authentication request is an authentication request of an evolved packet system architecture.

38. The method of claim **35**, wherein the authentication request message is received from a mobility management entity.

39. The method of claim **35**, wherein the authentication response message is transmitted to the mobility management entity.

40. The method of claim **35**, wherein the cellular terminal comprises a security entity that comprises a secure element and a subscriber identity module application.

41. The method of claim **40**, wherein the security entity is configured to decode authentication requests and to produce authentication responses.

42. The method of claim **35**, wherein the cryptographic algorithms are selected from a group consisting of MILENAGE; 128 bit TUAK; and 256 bit TUAK.

43. The method of claim **35**, wherein the failure report comprises an authentication failure message.

44. The method of claim **35**, wherein the authentication failure message comprises any of: a protocol discriminator; a security header type; an authentication failure message type; an EPS mobility management, EMM, cause; and an authentication failure parameter.

45. The method of claim **35**, wherein the cellular terminal is configured to produce the failure report in a manner dependent on the error that was likely to prevent successful decoding of the authentication request or the use of the selected cryptographic algorithm.

46. The method of claim **35**, wherein the cellular terminal is configured to detect an error in a message authenticator of the authentication requests, MAC-A.

47. The method of claim **46**, wherein the cellular terminal is configured to contain in the failure report, if the error was caused by incompatible length of MAC-A: an indication of the length of at least one of: the TUAK MAC-A used by the cellular terminal; and the TUAK MAC-A that the cellular terminal derives as likely used by the cellular network in the authentication request.

48. The method of claim **35**, wherein the failure report comprises a new information element for error reporting.

49. The method of claim **35**, wherein the cellular terminal is configured to detect an error in an authentication management field. The authentication management field is contained by the MAC-A.

50. The method of claim **49**, wherein the failure report indicates any one or more of: the length of TUAK MAC-A used by the cellular terminal; the length of TUAK MAC-A the cellular terminal presumes network used; the length of TUAK integrity key used by the cellular terminal; the length of TUAK integrity key the cellular terminal presumes network used; the length of TUAK cipher key used by the cellular terminal; the length of TUAK cipher key the cellular terminal presumes network used; the length of TUAK authentication value used by the cellular terminal; the length of TUAK authentication value; the cellular terminal presumes network used; the length of TUAK shared secret key used by the cellular terminal; and the length of TUAK shared secret key the cellular terminal presumes network used.

51. The method of claim **35**, wherein the cellular terminal is configured to detect an error in a re-synchronization token.

52. The method of claim **51**, wherein the failure report contains an indication of the re-synchronization token as computed by the cellular terminal.

53. A method in a cellular network, comprising:

receiving a request that requires authentication procedure triggering and responsively transmitting an authentication request message with an indication of a selected cryptographic algorithm from a group of a plurality of cryptographic algorithms;

receiving an authentication response message or a failure report indicative of a failure of the cellular terminal to produce an authentication response message corresponding to the authentication request message; and

adjusting cellular authentication process with the cellular terminal in response to receiving the failure report.

54. An apparatus comprising at least one memory and processor that are collectively configured to cause the apparatus to perform:

transmitting a request that requires authentication procedure triggering to a cellular network and responsively receiving from the cellular network an authentication request message with an indication of a selected cryptographic algorithm from a group of a plurality of cryptographic algorithms;

attempting to decode the authentication request message to a decoded authentication request according to the